UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

DEREK MICHAEL TAGG,

Defendant.
_____/

Cr. No. 16-20597
Honorable Paul D. Borman

Filed under seal

MOTION TO SUPPRESS EVIDENCE
SEIZED PURSUANT TO NIT SEARCH WARRANT

Defendant DEREK MICHAEL TAGG, through Counsel Jonathan Epstein and Benton Martin of the Federal Defender Office, moves to suppress evidence obtained pursuant to a search warrant issued February 20, 2015, in the Eastern District of Virginia, and in support states as follows:

1. Derek Tagg is charged in an Indictment with receipt and possession of child pornography. (R. 19, Indictment, Pg ID 59–60.)

2. The government has provided notice it may introduce evidence obtained from execution of two search warrants: one dated February 20, 2015, arising out of the Eastern District of Virginia (Ex. A, "NIT Warrant") and another dated September 15, 2015, issued out of this district, for the residence (Residential Search Warrant). (R. 24, Gov. Disc. Notice, Pg ID 85.)

2. In the February 20, 2015 NIT Warrant and Affidavit, FBI Special Agent Douglas MacFarlane sought authorization pursuant to Fed. R. Crim. P. 41

to deploy a "network investigative technique" (NIT) which involved modifying the code of a website hosted on a computer server in the Eastern District of Virginia to cause any computer logging in to the website to download certain software. That software then sent information about the computers to the FBI. (Ex. A.) The locations of the computers that might log in to the targeted website were unknown at the time Agent MacFarlane applied for the Warrant.

4. At least four courts have concluded that this same warrant is invalid and have suppressed the fruits of the search because the warrant exceeded the limits on the magistrate judge's authority under Rule 41(b). *See United States v. Croghan,* No. 1:15-CR-48, 2016 WL 4992105 (S.D. Iowa Sept. 19, 2016); *United States v. Workman,* No. 15-CV-00397-RBJ-1, 2016 WL 5791209, at *4 (D. Colo. Sept. 6, 2016); *United States v. Levin*, No. CR 15-10271-WGY, 2016 WL 2596010 (D. Mass. Apr. 20, 2016); *United States v. Arterbury*, No. 15-CR-182-JHP, ECF Doc. 42 (N.D. Okla. Apr. 25, 2016); *but see, e.g., United States v. Broy,* No. 16-CR-10030, 2016 WL 5172853, at *7 (C.D. Ill. Sept. 21, 2016); *United States v. Jean,* No. 5:15-CR-50087-001, 2016 WL 4771096 (W.D. Ark. Sept. 13, 2016); *United States v. Stamper,* No. 1:15CR109, 2016 WL 695660 (S.D. Ohio Feb. 19, 2016); *United States v. Michaud*, No. 3:15-cr-05351-RJB, 2016 WL 337263 at *4–5 (W.D. Wash. Jan. 28, 2016).

5. Other courts have reached similar conclusions in regard to other warrants that exceed the jurisdictional limitations of Rule 41(b). *See United States v. Martin,* No. 15-20544-02, 2016 WL 4493675 (E.D. Mich. Aug. 26, 2016); *United States v. Barber*, No. 15-40043-CM, 2016 WL 1660534, at *3–4 (D. Kan. Apr. 27, 2016); *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 756–58 (S.D. Tex. 2013).

6. Further, the NIT Warrant and Affidavit also failed to satisfy the particularity requirement of the Fourth Amendment. *See In re Warrant*, 958 F. Supp. 2d at 758–59.

7. As a result of these violations, all evidence obtained from the NIT search should be suppressed. Additionally, a subsequent search of the residence issued based on evidence from the NIT search, should be suppressed as fruit of the poisonous tree. (Ex. B, Residential Search Warrant.)

8. The government does not concur in the requested relief.

WHEREFORE, Defendant Tagg asks this Court to suppress all evidence obtained from the search authorized in the February 20, 2015 NIT Warrant, along with additional evidence from the subsequent residential search of the home as fruit of the poisonous tree.

Respectfully Submitted,

FEDERAL DEFENDER OFFICE

s/Jonathan M. Epstein
jonathan_epstein@fd.org

s/Benton C. Martin
benton_martin@fd.org

Attorneys for Defendant
613 Abbott St., 5th Floor
Detroit, MI 48226
Phone: 313-967-5542

Dated: October 11, 2016

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

DEREK MICHAEL TAGG,

Defendant.
_____/

Cr. No. 16-20597
Honorable Paul D. Borman

Filed under seal

MEMORANDUM IN SUPPORT OF MOTION TO SUPPRESS EVIDENCE SEIZED PURSUANT TO NIT SEARCH WARRANT

On February 20, 2015, a magistrate judge in the Eastern District of Virginia signed a warrant application authorizing the FBI to engage in an unprecedented computer hacking operation to sweep up information about computers used to log in to a Tor-based website named Playpen. (*See* Ex. A, NIT Warrant.) The evidence from the illegal search led to a further search of residential homes. (Ex. B, Residential Warrant.) Through these searches, the government obtained evidence it intends to use against Mr. Tagg at trial.

Mr. Tagg urges this Court to follow other courts in suppressing the evidence from this search on the basis that the warrant ran afoul of the limits on magistrate judge authority in Fed. R. Crim. P. 41(b) and 28 U.S.C. § 636. *See United States v. Croghan,* No. 1:15-CR-48, 2016 WL 4992105 (S.D. Iowa Sept. 19, 2016); *United*

States v. Workman, No. 15-CV-00397, 2016 WL 5791209, at *4 (D. Colo. Sept. 6, 2016); *United States v. Levin*, No. CR 15-10271, 2016 WL 2596010 (D. Mass. Apr. 20, 2016); *United States v. Arterbury*, No. 15-CR-182, ECF Doc. 42 (N.D. Okla. Apr. 25, 2016). Courts have reached similar conclusions regarding other warrants that violated Rule 41(b)'s limits. *See United States v. Martin,* No. 15-20544-02, 2016 WL 4493675 (E.D. Mich. Aug. 26, 2016); *United States v. Barber*, No. 15-40043, 2016 WL 1660534, at *3–4 (D. Kan. Apr. 27, 2016); *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 756–58 (S.D. Tex. 2013). Similarly, all fruit of the search here must be suppressed.

Background

A. Government Seizure and Control of the Targeted Website

The Playpen website operated using "The Onion Router" or "Tor" software, which the U.S. government developed to enable anonymous communications. (Ex. A, ¶¶ 6–7.) The software is publicly available and free to download. It operates by routing communications through a series of computers to mask the user's actual IP address. When a Tor user visits a website, the only IP address that appears in the website's log is that of a Tor "exit node," i.e., "the last computer through which a user's communications were routed." (*Id.* ¶ 8.) Thus, for Tor users, "traditional IP identification techniques are not viable." (*Id.*) The targeted website in this case could purportedly only be accessed by Tor users. (*Id.* ¶ 10.)

According to the Affidavit, in December 2014, a foreign law enforcement agency contacted the FBI with information that a U.S.-based IP address may be associated with Playpen. (*Id.* ¶ 28.) After that, FBI officials discovered a copy of the Playpen website resided on a server hosted by a company in North Carolina, and the agency seized the server. (*Id.*) FBI agents next searched the Florida residence of Playpen's suspected administrator and "assumed administrative control" of the website. (*Id.* ¶¶ 28, 30.) The FBI then continued operating Playpen, facilitating the distribution of child pornography, from a "government-controlled computer server" in the Eastern District of Virginia. (*Id.*)

B. Authorization for Network Investigative Technique (NIT)

Through the warrant, Agent MacFarlane sought authorization to deploy a "network investigative technique" (NIT) using this government-controlled server in Virginia. (*Id.* ¶ 31.) The application stated that the FBI planned to "augment" Playpen's code so that certain software was delivered to the computers of visitors who accessed the website. (*Id.* ¶ 33.) The software then caused the computer to transmit to the FBI the computer's actual IP address, the type of operating system on the computer (e.g., Windows 7), the computer's host name, the active username, and the Media Access Control (MAC) address. (*Id.* ¶ 34.) Experts describe the NIT as "malware," since it exploits software vulnerabilities to

circumvent Tor's anonymity protections.[1] The technique is called a "watering hole attack," since "every visitor of the hacked site or server gets infected with the malware."[2]

Law and Argument

I. The Warrant Application Exceeded Rule 41(b)'s Territorial Limits.

The warrant here was purportedly authorized under the magistrate judge's authority under 28 U.S.C. § 636 and Fed. R. Crim. P. 41(b). (Ex. A, Cover Page.) But under Rule 41(b), there are territorial limits on a magistrate judge's authority to issue a warrant. The rule provides five alternative bases for that authority, and only subsections (1), (2), and (4) are even arguably applicable here:

> (1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district;
>
> (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

---

[1] *See* Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, Wired, Aug. 5, 2014, *available at* http://www.wired.com/2014/08/operation_torpedo/.

[2] Lorenzo Franceschi-Bicchierai, *The FBI Hacked a Dark Web Child Porn Site to Unmask Its Visitors*, Motherboard, July 15, 2015, *available at* http://motherboard.vice.com/read/the-fbi-hacked-a-dark-web-child-porn-site-to-unmask-its-visitors.

> . . .
> (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; . . . .

Fed. R. Crim. P. 41(b)(1)–(2). "Property" includes "documents, books, papers, any other tangible objects, and information." Fed. R. Crim. P. 41(a)(2)(A).

The application here did not meet any of these provisions. Although the government used a server in the Eastern District of Virginia to deliver the NIT software, that software was downloaded by computers of unknown location. Once downloaded, the software caused a search of the computer from the location of the person who had visited the targeted website. Although the government has argued in other cases that Rule 41(b) may be flexible enough to cover this operation, the clear majority of courts have concluded that the magistrate judge lacked authority to authorize this remote search for information on computers of unknown location. [3]

---

[3] *See United States v. Broy,* No. 16-CR-10030, 2016 WL 5172853, at *8 (C.D. Ill. Sept. 21, 2016); *Croghan*, 2016 WL 4992105, at *1; *United States v. Knowles*, No. 15-cr-875 (D. S.C. Sep. 14, 2016); *United States v. Ammons*, No. 3:16-CR-00011-TBR-DW, 2016 WL 4926438, at *6 (W.D. Ky. Sept. 14, 2016); *United States v. Torres*, No. 16-cr-285 (W.D. Tex. Sep. 9, 2016); *United States v. Workman*, No. 15-cr-397 (D. Co. Sep. 6, 2016); *United States v. Henderson*, No. 15-cr-565 (N.D. Cal. Sep. 1, 2016); *United States v. Adams*, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *6 (M.D. Fla. Aug. 10, 2016); *United States v. Acevedo-Lemus*, No. 15-00137-CJC, 2016 WL 4208436 (C.D. Cal. Aug. 8, 2016); *United States v. Rivera*, No. 2:15-cr-266-CJB-KWR (E.D. La. Jul. 20, 2016); *United States v.*

As to Rule 41(b)(1), the government has suggested in other cases that the provision applies because (1) the NIT was deployed in Virginia and returned the information it collected to that district, or (2) the information was first examined in Virginia. But that is not what the rule allows. Under Rule 41(b)(1), the information must be "located within the district." If this applies whenever information is first viewed in the district, then "a Rule 41 warrant would permit FBI agents to roam the world in search of a container of contraband, so long as the container is not opened until the agents haul it off to the issuing district." *In re Warrant*, 958 F. Supp. 2d at 757. This stretches the territorial limits of Rule 41(b)(1) too far. *Id.* Likewise, as explained in *Levin*, the government's position that the search occurred in Virginia, rather than the individual computers the information was collected from, is "nothing but a strained, after-the-fact rationalization." 2016 WL 2596010, at *5. In this case, the object of the government's search was specific information stored on Mr. Tagg's computer, and nothing shows that this information ever entered Virginia until after the government hacked Tagg's computer.

Nor does Rule 41(b)(2) apply. *See, e.g., Levin*, 2016 WL 2596010, at *6; *Michaud*, 2016 WL 337263, at *6. Rule 41(b)(2) expressly addresses transient

---

Werdene, No. 15-CR-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016); *United States v. Arterbury*, No. 15-CR-182-JHP (N.D. Okla. May 17, 2016); *Levin*, 2016 WL 2596010; *United States v. Stamper*, No. 1:15CR109, 2016 WL 695660 (S.D. Ohio Feb. 19, 2016); *Michaud*, 2016 WL 337263.

information first located in the district that may be moved after the warrant is issued, whereas the information here was stored at unknown, out-of-district locations at the time the warrant issued. The FBI caused the NIT software to be downloaded to the users' local computers—where the search occurred—and the NIT software then sent data to the FBI. Rule 41(b)(2) does not authorize warrants "for property *outside* the district when the warrant is issued, but brought back inside the district before the warrant is executed." *In re Warrant*, 958 F. Supp. 2d at 757.

Finally, courts have soundly rejected Rule 41(b)(4)'s application to this warrant. *See, e.g., Croghan,* 2016 WL 4992105, at *4–5*; Levin*, 2016 WL 2596010, at *6; *Arterbury*, ECF Doc. 42, at 16–17; *Michaud*, 2016 WL 337263, at *6. Rule 41 defines "tracking device" as one that "'permits the tracking of the movement of a person or object.'" *Croghan,* 2016 WL 4992105, at *4 (citing Fed. R. Crim. P. 41(a)(2)(E)). But the NIT "did not 'track' the 'movement' of anything; rather, it caused computer code to be installed on the activating user's computer, which then caused such computer to relay specific information to the government-controlled computers in Virginia." *Id.* Moreover, Rule 41(b)(4) requires installation of the tracking device "within the district." Here, the FBI modified the code of the target website to cause any computer visiting the site to download the NIT software. Thus, the warrant anticipates installation of the NIT software *outside* of

the district. In fact, as in *In re Warrant*, 958 F. Supp. 2d at 758, "the software would be installed on a computer whose location could be anywhere on the planet."

The fact that Rule 41(b) does not extend to extraterritorial searches should have been well known to the government. Notably, at least partially in response to the ruling in *In re Warrant*, DOJ proposed amending Rule 41 to allow judges to issue warrants like the one here, when the government seeks electronically stored data from devices of unknown location. *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326, 356–57 (2015). Even if approved, the amendment raises concerns of extraterritorial searches. As many as 80% of Tor users "connect to the network from outside the United States." *Id.* at 357. And "even when a targeted device is located territorially, the data accessed from the device may be stored extraterritorially." *Id.* There is no authority for U.S. judges to authorize surreptitious downloads of U.S.-government spyware to devices in foreign countries.

II. The Warrant Violates the Fourth Amendment Particularity Requirement.

"[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched, and the persons or things to be seized*." U.S. Const., Amend IV (emphasis added). "The chief purpose of the particularity requirement is to prevent general searches by requiring a neutral judicial officer to cabin the scope of the search to those areas and items

for which there exists probable cause that a crime has been committed." *United States v. Richards*, 659 F.3d 527, 537 (6th Cir. 2011) (quotation and alteration omitted).

The warrant application here failed to explain how the government planned to particularize its search to only those suspects engaging in criminal activity on Playpen. *See In re Warrant*, 958 F. Supp. 2d at 759 (rejecting similar NIT warrant on particularity grounds). Professor Orin Kerr recently criticized courts' failure to recognize the significance of the particularly problem raised by this extremely broad description. Exhibit C, Orin Kerr, *Government 'hacking' and the Playpen search warrant*, Volokh Conspiracy, Sept. 27, 2016).[4] He emphasized that, although courts have at times approved warrants involving the monitoring of a *single* suspect or *single* device that may move to an unknown location, "the Playpen warrant authorized searching an unlimited number of computers located all around the world." *Id.* "The place to be searched was not wherever a single suspect went, or a single item of property, but rather thousands of machines located throughout the planet . . . in an automated process." *Id.*; *see* Brian L. Owsley, *Beware of Government Agents Bearing Trojan Horses*, 48 Akron L. Rev.

[4] http://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/09/27/government-hacking-and-the-playpen-search-warrant/.

315, 347 (2015) (warning judges to account for likelihood a search may sweep up third party data).

Furthermore, it is now clear that the FBI *could have* made this search more particular. According to an FBI agent's testimony, when the FBI was operating Playpen, agents were able to monitor and capture the activity of each individual user. Exhibit D, *United States v. Matish*, 16-cr-16, Mot. Hrg., at 7–8 (June 14, 3016). The government could have used this evidence to obtain individual NIT warrants against particular users who had accessed child pornography on the site. But instead of using this targeted approach, the government opted to search the computer of anyone in the world who simply logged into the site—even if that user logged out immediately without viewing any child pornography. This procedure violated the particularly requirement of the Fourth Amendment.[5]

[5] The government in other cases has contested whether this collection of IP addresses constituted a search at all. But the majority of courts have rejected that argument. *See, e.g., Croghan*, 2016 WL 4992105, at *4; *Broy*, 2016 WL 5172853, at *5–6; *United States v. Darby*, No. 2:16CR36, 2016 WL 3189703, at *5–6 (E.D. Va. June 3, 2016). Relying on *Riley v. California*, 134 S. Ct. 2473, 2480 (2014), the courts have held that when, as here, an IP address is collected directly from a personal computer, rather than from a third party, a search occurs. *Croghan*, 2016 WL 4992105, at *7. In *Riley*, notably, the Supreme Court rejected the argument that officers should be allowed to look at telephone numbers in a cell phone's call logs incident to arrest, despite the fact that those numbers are voluntarily shared with a third party when dialed. 134 S. Ct. at 2492–93. Moreover, it is important to distinguish Tor users from general Internet users; the Tor Project promotes Tor as preventing the sharing of IP addresses. Thus, Tor users retain a reasonable expectation of privacy in their IP addresses that other Internet users do not. Additionally, the search here collected not only IP addresses but also other

III. Suppression is warranted as a remedy.

1. Violations of Rule 41(b)(1)'s jurisdictional limits warrant suppression.

The Sixth Circuit has recognized that suppression may be the appropriate remedy when agents obtain a warrant from a judge who lacked authority to issue it. *See United States v. Master*, 614 F.3d 236 (6th Cir. 2010). In *Master*, the court relied on *Herring v. United States*, 555 U.S. 135 (2009), to explain that the good faith exception cannot salvage a search when the police conduct was sufficiently deliberate that exclusion could deter it. The court explained: "Intentional attempts to avoid adhering to jurisdictional limitations imposed by state law is conduct that can and should be considered and deterred by the judiciary." *Id.* at 243. Moreover, the court upheld the outcome, though not the reasoning, of its earlier decision in *United States v. Scott*, 260 F.3d 512 (6th Cir. 2001), which upheld exclusion of evidence when "officers made at best minimal attempts to find available, active magistrates before presenting the warrant to [a] retired judge" who lacked authority to issue the warrant. *Master*, 614 F.3d at 242 n.3.

Here, the good-faith inquiry falls squarely in favor of excluding the fruits of the NIT search. An experienced FBI agent ignored the clear limitations of Rule 41(b), despite the government having been criticized in 2013, in *In re Warrant*, 958

---

identifying information such as usernames and MAC addresses, which are not shared with third parties and for which Tagg never lost his expectation of privacy.

F. Supp.2d at 756–57, for failing to do so. A suppression ruling here would serve the exclusionary rule's purposes of deterring "deliberate, reckless, or grossly negligent conduct" and "recurring or systemic negligence." *Herring*, 555 U.S. at 144. In particular, suppression would deter deliberate and systemic violations of Rule 41(b).

Other courts have relied on these same grounds to exclude the evidence gathered using the same NIT warrant at issue here. *See Croghan*, 2016 WL 4992105, at *8; *Levin*, 2016 WL 2596010, at *13; *Workman*, 2016 WL 5791209, at *8; *Arterbury*, No. 15-cr-182, ECF Doc. 42, at 25. *Workman* and *Arterbury* focused on the distinction between technical and substantive violations of Rule 41, and held that good faith does not excuse violations of Rule 41 that implicate substantive judicial authority. *See Workman*, 2016 WL 5791209, at *8.

The court in *Levin* expanded on this point, giving the following additional explanation for why good faith should not apply:

> For one, it was not objectively reasonable for law enforcement—particularly "a veteran FBI agent with 19 years of federal law enforcement experience[,]" Gov't's Resp. 7-8—to believe that the NIT Warrant was properly issued considering the plain mandate of Rule 41(b). *See Glover*, 736 F.3d at 516 ("[I]t is quite a stretch to label the government's actions in seeking a warrant so clearly in violation of Rule 41 as motivated by 'good faith.'"); *cf. United States v. McKeever*, 894 F.2d 712, 717 (5th Cir. 1990) (good-faith exception did not apply where sheriff "who was the prime mover in obtaining and executing the search ... knew both that he had to obtain a warrant from a court of record ... and that [the issuing judge] was not a judge of a court of record."). Moreover, even analyzed under *Herring*, the conduct at

> issue here can be described as "systemic error or reckless disregard of constitutional requirements," 555 U.S. at 147, 129 S. Ct. 695, and the Court thus concludes that suppression is appropriate.

Levin, 2016 WL 2596010, at *13.

The *Croghan* court similarly concluded that suppression is the appropriate remedy, no matter whether the warrant's defect is categorized as a "technical" or "substantive" violation of Rule 41(b):

> Suppression is an appropriate means to deter law enforcement from seeking warrants from judges lacking jurisdiction to issue them, and this deterrence function outweighs the societal costs associated with suppression. Moreover, the Court finds that law enforcement was sufficiently experienced, and that there existed adequate case law casting doubt on magisterial authority to issue precisely this type of NIT Warrant, that the good faith exception is inapplicable.

2016 WL 4992105, at *8.

Levin relied in part on *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015), which further supports suppression. There, an agent applied for a warrant in a federal court in Kansas to search for a cellphone and computer he had learned were in Oklahoma. *Id.* at 1111. On appeal, the government argued that the Rule 41 violation did not prejudice the defendant because an Oklahoma court *could have* authorized the warrant. *Id.* at 1114–15. The Tenth Circuit disagreed, warning that "[w]hen it comes to something as basic as who can issue a warrant, we simply cannot accept such a speculative approach." *Id.* at 1116. Thus, even assuming the warrant did not violate the Fourth Amendment, the court affirmed the suppression

ruling. *Id*. at 1117. The court explained that suppression "further[ed] the purpose of the exclusionary rule by deterring law enforcement from seeking and obtaining warrants that clearly violate Rule 41(b)(1)." *Id.*

The D.C. Circuit has likewise held that a warrant violating Rule 41(b)'s territorial limitations could not be "excused as a 'technical defect.'" *United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2013). The court explained that it could "not see how a blatant disregard of a district judge's jurisdictional limitation can be regarded as only 'technical.'" *Id.* (reversing based on failure to suppress).

Another judge in this district recently suppressed evidence based on a similar violation of Rule 41(b)'s territorial limitations. *United States v. Martin*, No. 15-20544-02, 2016 WL 4493675 (E.D. Mich. Aug. 26, 2016). In *Martin*, ATF agents obtained a Rule 41(b)(4) tracking warrant from a state judge rather than federal judge. *Id.* at *3. The court first determined that the agents ran afoul of the jurisdictional limits in Rule 41(b). *Id.* The court then concluded that suppression was proper in order to deter future violations of the rule. *Id.* at *4. The court noted that the government failed to show that a federal magistrate judge was unavailable, and that the prosecutor admitted that this procedure had occurred before. *Id.*

This Court should reject the approach of those courts to uphold this warrant on grounds of good faith. In *Michaud*, 2016 WL 337263, at *6, for example, the court recognized that the warrant ran afoul of Rule 41(b) but court relied on

decisions addressing "technical" Rule 41 violations, rather than violations of Rule 41(b)(1), to permit the government to use the evidence seized. *See, e.g., United States v. Weiland*, 420 F.3d 1062, 1071 (9th Cir. 2005) (addressing alleged Rule 41(b) violation based on the fact that a state, not federal, official applied for the warrant); *United States v. Welch*, 811 F.3d 275, 279–81 (8th Cir.), *cert. denied*, 136 S. Ct. 2476 (2016) (refusing to suppress when agents ran afoul of Rule 41's requirement to provide notice of warrant within 30 days). *Krueger* specifically distinguished these type of "technical" Rule 41 violations on the basis that such violations do not implicate "substantive judicial authority." 809 F.3d at 1115 n.7. Similarly, the D.C. Circuit in *Glover* warned that "it is quite a stretch" to view agents' seeking a warrant in violation of Rule 41 territorial limitations "as motivated by 'good faith.'" 736 F.3d at 516.

This case presents strong justification for suppression. First, there is no evidence the government sought to take this warrant to a district judge, and there is evidence that this type of investigation has been conducted before. Moreover, the government was clearly aware of the limitations of Rule 41(b) before this search, as shown by the DOJ's efforts to amend Rule 41. The Advisory Committee record on the proposed changes belies any assertion that the DOJ is merely seeking a clarifying amendment. The Committee endorsed amending the rule only after "intense debate." *See* Zach Lerner, *A Warrant to Hack: An Analysis of the*

Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure, 18 Yale J. L. & Tech. 26, 36 (2016). The Committee also refused to adopt "broader language relaxing [Rule 41's] territorial restrictions," ultimately recommending a "narrowly tailored" exception to Rule 41(b) for crimes involving anonymizing software.[6] Further, the Committee declined to address "constitutional questions that may be raised by warrants for remote electronic searches, such as the specificity of description that the Fourth Amendment may require in a warrant for remotely searching electronic storage media or seizing or copying electronically stored information."[7]

The FBI failed to notify the magistrate judge here to this serious, ongoing debate about the limitations of Rule 41(b) and the Fourth Amendment. The warrant represents reckless disregard of the limitations on magistrate-judge authority, and the evidence must be suppressed.

2. Violation of the Particularity Clause Warrants Suppression.

[6] Memorandum from Hon. Reena Raggi, Advisory Comm. on Criminal Rules, on the Report of the Advisory Committee of Criminal Rules to Hon. Jeffrey S. Sutton, Chair, Comm. on Rules of Practice and Procedure (May 5, 2014), in Comm. on Rules of Practice and Procedure of the Judicial Conference of the U.S., Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure: Request for Comment 326 (Aug. 2014), https://perma.cc/9ZJW-GRRC.

[7] *Id.*

The Supreme Court has repeatedly recognized that "'a warrant may be so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.'" *Groh v. Ramirez*, 540 U.S. 551, 565 (2004) (quoting *United States v. Leon*, 468 U.S. 897, 923 (1984)). Further, an officer's restraint in conducting a search cannot cure a violation of the Fourth Amendment's particularity requirement. *See id.* at 561–63; *United States v. Lazar*, 604 F.3d 230, 237 (6th Cir. 2010). The Sixth Circuit refuses to apply the good faith exception when a warrant is overbroad on its face, particularly if the agent could have provided narrower limits in the warrant. *See Lazar*, 604 F.3d at 238 (upholding suppression ruling when government used overbroad descriptive terms in describing patient files to be seized); *United States v. Ford*, 184 F.3d 566, 575–78 (6th Cir. 1999) (finding Fourth Amendment violation when warrant failed to limit scope of search when limits were reasonably available).

Here, the warrant authorized intrusive searches of any devices used to log in to the targeted website, even if that user immediately left the site after receiving what it contained. Additionally, Playpen contained chat forums and erotic fiction sub-forums that could be used without viewing child pornography. Even more troublingly, when the FBI was running Playpen, it could observe the activity of specific users, and it could see which users visited which parts of the website. Yet

instead of obtaining warrants for specific users, the government swept every single user who logged into the site. A reasonable officer would have recognized this sweeping authorization as a violation of the particularity requirement.

3. Suppression is warranted because the warrant contained material statements in support of probable cause made with reckless disregard for the truth.

Under *United States v. Leon*, 468 U.S. 897 (1984), and *Franks v. Delaware*, 438 U.S. 154 (1978), suppression "remains an appropriate remedy if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth." *Leon*, 468 U.S. at 923. Here, the warrant contained material statements made with reckless disregard for their truth.

First, the warrant's application provided a false description of Playpen's home page as it existed at the time. The application states that Playpen's main page depicts "two images depicting partially clothed prepubescent girls with their legs spread apart." (Ex. A, ¶ 10.) The affiant further claimed that these images contributed to "probable cause to believe that . . . any user who successfully accesses [Playpen] has knowingly accessed with intent to view child pornography, or attempted to do so." (*Id.*) A screen shot of this version of the home page has been made public in one of the cases stemming from the search.

See United States v. Michaud, No. 15-cr-5351, ECF Doc. 90-1, at 2 (W.D. Wash. Dec. 21, 2015).

By the time of the warrant application, however, Playpen's original administrator had changed the home page to a much less suggestive image. *See Michaud*, No. 15-cr-5351, ECF Doc. 90, at 3 (W.D. Wash. Dec. 21, 2015) (government filing admitting home page change). The revised home page shows a single image of a clothed female with her legs crossed. The image is small and it is not clear at first glance that she is under age 18. A special agent involved in the Florida search has conceded that he saw the new home page before the warrant application was submitted but did not alert the magistrate judge to this change. (Ex. C, Mot. Hrg., Jan. 22, 2016, *United States v. Michaud*, at 92.)

This change is significant because the warrant application emphasized the nature of the image on the *old home page* in support of probable cause to search any computer used to log in to Playpen. The FBI sought to use the NIT on any "activating computers," defined as the computers of "any user or administrator who logs into the TARGET WEBSITE by entering a username and password." (Ex. A, Warrant Attachment A.) A username and password could be made up and entered without verification or other steps, and the site was free. Thus, Playpen's initial appearance and accessibility gave no clear indication of its criminal uses. Whether a website "unabashedly announce[s]" that its purpose is to trade child

pornography when assessing whether a search warrant affidavit established probable cause. *See, e.g., United States v. Shields,* 458 F.3d 269, 279 (3d Cir. 2006); *United States v. Martin*, 426 F.3d 68, 75 (2d Cir. 2005).[8]

The warrant also incorrectly described Playpen as being dedicated in its "entirety" to child pornography. (Ex. A, ¶ 27). In fact, as the government has conceded in other cases, the website contained a chat forum and sub-directories devoted to erotic fiction without any images. As to the chat forum and erotic fiction, the magistrate judge should have been allowed to consider the possible First Amendment implications when determining how much authority to allow the FBI in targeting visitors to the site.

Additionally, the warrant affidavit incorrectly described Playpen's accessibility. The affidavit claims that "Tor hidden services are not indexed like websites on the traditional Internet" because "unlike on the traditional Internet, a user may not simply perform a Google search for the name of one of the websites on Tor to obtain and click on a link to the site." (Ex. A, ¶ 10.) The affiant thus asserted, in support of probable cause, that it was "extremely unlikely that any user could simple stumble upon [Playpen] without understanding its purpose and

[8] The name "Playpen" is not necessarily indicative of child pornography, as it is also the name of multiple legitimate adult strip clubs and is a popular name for fictional adult pornography magazines (as a takeoff of Playboy). *See, e.g.*, Wikipedia, List of Fictional Magazines, https://en.wikipedia.org/wiki/List_of_fictional_magazines.

content." (*Id.*) In fact, however, for most Tor users, the general approach to accessing the so-called "Deep Web" *is* through search engines. *See* Exhibit E, Daniel Sui, *et al.*, *The Deep Web and the Darknet*, The Wilson Center 7 (2015), *available at* https://www.wilsoncenter.org/sites/default/files/stip_dark_web.pdf; Exhibit F, Bret Hawkins, *Under The Ocean of the Internet – The Deep Web* 7 (2016), *available at* https://www.sans.org/reading-room/whitepapers/covert/ocean-internet-deep-web-37012 (noting that "there are plenty of search engines that allow you to search databases not indexed by the Google's and Bing's of the world"). The affidavit made no mention of the availability of these services.

The Second Circuit's recent decision in *United States v. Raymonda*, 780 F.3d 105, 115 (2d Cir.), *cert. denied*, 136 S. Ct. 433 (2015), underscores why the omission of this information is materially misleading. There, the court found a warrant lacked probable cause to search a person's home based on information he accessed a child-pornography website when the information "was at least equally consistent with an innocent user inadvertently stumbling upon a child pornography website, being horrified at what he saw, and promptly closing the window." *Id.* at 117. In prior cases, the series of steps taken to access child pornography was used to suggest willful intent to seek child pornography. *Id.* at 115. In contrast, "the mere fact [a] defendant had apparently tried to access a

non-membership website featuring images of child pornography, absent any evidence that he subsequently viewed those images, did not establish probable cause to search his computer." *Id.* at 116. In light of this case law, the affiant's misleading statements about the steps a person needed to take to access Playpen cannot fairly be described as immaterial.

Further, the warrant application's cover page—in designating the location of the property to be searched as solely being in the Eastern District of Virginia—left off critical information. (*See* Ex. A, Cover Page.) In stark contrast, in prior (more limited) NIT warrant applications, the government appended "and elsewhere" to the description of the place to be searched. *See United States v. Cottom*, No. 13-cr-108, ECF Doc. 122-1 (D. Neb. Apr. 16, 2014); *In re Search of Email Address texas.slayer@yahoo.com*, No. 12-sw-5685, ECF Doc. 4 (D. Colo. Oct. 19, 2012). Those prior warrants appropriately notified the magistrate judge of the fact that the search encompassed locations outside of the judge's district. This practice appears to have changed after *In re Warrant*, in which the magistrate judge denied the government's NIT request as failing to comply with the Fourth Amendment and Rule 41(b). Only after that decision did the DOJ begin advocating to amend Rule 41(b) to permit searches for property "elsewhere" than the issuing district. That the FBI dropped this phrase from the face of this warrant suggests it sought to avoid red flags about the (at best) questionable legality of this operation.

Moreover, the affidavit did not clearly explain how the NIT operated. The affidavit falsely stated that the NIT simply piggybacks on the content users of Playpen would already download during the website's "normal course of operation." (Ex. A, ¶ 33.) But it is now apparent the government used an "exploit" to hack into Playpen users' computer. Further, the affidavit did not disclose any limit on how long the NIT software would remain on the affected computers, and although the affidavit claimed that it listed all information that would be revealed to the government, it did not state clearly whether this information would be transmitted only once or on an ongoing basis.

The omissions in the NIT warrant fatally undermine probable cause for the NIT search. All it took to trigger the search was for a Tor user to find Playpen through a search engine and log in through the home page. Even if that user left the site immediately after realizing it contained illicit content, the search was still performed. Accordingly, through use of false statements, the FBI was able to gloss over the fact that its operation failed to account for the possibility of searching the computers of innocent Tor users and would impermissibly swept up information for which no probable cause existed. For that reason, this Court should refuse to apply the good-faith exception to the exclusionary rule.

Conclusion

Tagg asks the Court to suppress all evidence obtained through the search in the February 20, 2015 warrant, and any evidence obtained from additional searches authorized through use of evidence from the initial illegal search including all incriminating statements as fruit of the poisonous tree.

Respectfully Submitted,

FEDERAL DEFENDER OFFICE

s/Jonathan M. Epstein
jonathan_epstein@fd.org

s/Benton C. Martin
benton_martin@fd.org

Attorneys for Defendant
613 Abbott St., 5th Floor
Detroit, MI 48226
Phone: 313-967-5542

Dated: October 11, 2016

CERTIFICATE OF SERVICE

Counsel certifies that on the above date, the foregoing paper was filed under seal with the clerk of the Court using the ECF system, and a copy of this motion will be mailed to opposing counsel in a manner consistent with the rules for sealed filings.

s/Benton C. Martin